MULTIMEDIA UNIVERSITY

STUDENT ID NO

□□□□□□□□□□

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 1, 2017/2018

TAC3121 – APPLIED CRYPTOGRAPHY

(All sections / Groups)

14 OCTOBER 2017
9.00 a.m. - 11.00 a.m.
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This question paper consists of 3 pages including the cover page with **FIVE** questions only.

2. Attempt **ALL** questions. All questions carry equal marks and the distribution of the marks for each question is given.

3. Please print all your answers in the Answer Booklet provided.

Question 1

(a) Public key cryptography is developed to address TWO key issues in private key cryptography. Please state and describe the TWO issues. [2 marks]

(b) Describe the public key certification process and the corresponding verification process. [3 marks]

(c) What is a transposition cipher? Give TWO examples. [3 marks]

(d) State Fermat's Theorem, and use it to compute 5^{100} modulo 7. [4 marks]

Question 2

(a) Assuming you can do 10^6 decryptions per micro second and the key size is 256 bits, how long would a brute force attack take (state in years)? [3 marks]

(b) Decrypt the ciphertext "UKQ WNA CNAWP" using Caesar cipher with key $K = 4$. [3 marks]

(c) Construct a Playfair matrix with the keyword "SUCCESSFUL". Thus, decrypt the ciphertext "DTUDRNKHLEAMUECUUHMDLU". [6 marks]

Question 3

(a) Given that Bob has public RSA key $n = 65$, $e = 5$.

i. Verify that Bob's private key is $d = 29$. [3 marks]

ii. Alice wants to send the message $m = 7$ to Bob. What is the ciphertext? [2 marks]

(b) Consider a scenario that an adversary Eve has a ciphertext $C = (c_1, c_2) = (g^k, my^k)$ mod p encrypted using El Gamal encryption which she has eavesdropped or intercepted from a previous confidential communication between Alice and Bob. Eve will be able to learn the corresponding plaintext given the ciphertext. Show the steps that Eve is required to perform in order to retrieve the corresponding plaintext. [4 marks]

Continued...

(c) Alice and Bob wish to exchange a session key using the Diffie-Hellman key exchange protocol. They have agreed to use prime modulus q = 17 and generator α = 2. Alice chooses a secret number a = 3 and Bob chooses a secret number b = 5. What is the value of the session key that they generate? [3 marks]

Question 4

(a) State the purpose of S-boxes in Data Encryption Standard (DES)? [2 marks]

(b) State the outputs of the DES S-box S_2 upon applying the inputs 110010 and 011011 respectively. [4 marks]

S_2															
15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

(c) Describe how a meet-in-the-middle attack is possible against double-DES. [2 marks]

(d) State the FIVE modes of operation for block cipher. Which modes do not require the use of decryption algorithm in the decryption process? [4 marks]

Question 5

(a) List and describe the THREE adversarial capabilities and the THREE adversarial goals for a digital signature scheme. Which combination provides the most desirable security notion? [6 marks]

(b) What is the difference between a message authentication code and a one-way hash function? [3 marks]

(c) A digital signature and a message authentication code (MAC) both provide data integrity. A digital signature also provides non-repudiation, while a MAC does not. Why not? [3 marks]

End of Page